Information Acceptable Use Policy

Policy for acceptable use of OU information

An Open University Information Security Common Policy

Open University – Information Security Team

Information Classification: Internal use only
Purpose

This policy defines the acceptable use of information in order to protect students, research participant, staff and other confidential data and the university's information systems.

Overview

The Information Acceptable Use Policy covers general secure practice for information handling and should be read in conjunction with the other IT Security Policies.

Technical terms used within this document are defined in Appendix A.

It is the responsibility of every computer user to know and follow this policy.

Scope

All users of OU information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1. Information security classification

1.1 Data owners are responsible for defining the classification of their Open University information so that appropriate controls can be applied (See Information classification policy).

1.2 Data users must apply and abide by the controls defined within the appropriate Information Security Specific policy when processing or storing this information.

1.3 Information assets classified as Highly Confidential must be marked with the information security classification.

2. Information storage and transmission

2.1 Unless otherwise approved by IT, information must be stored on Central University Storage, ensuring availability and effective secure storage.

2.2 When exchanging confidential information with a 3rd party, you must ensure that it is conveyed securely. Seek advice from the IT Information Security Team if you are unsure how to do this or which standard needs to be followed.

3. Use of confidential information

3.1 Information should be treated as confidential unless declared otherwise by the data owner.
3.2 Do not forward, send or disseminate confidential information in any way that may compromise The Open University or its students. If in doubt speak to your line manager or the data owner.

4. Data Protection Act

4.1 The University is subject to UK legislation including the Data Protection and Freedom of Information Acts. It is therefore essential that you also adhere to the university Data Protection Code of Practice.

5. Information retention

5.1 The Open University has an information Retention Schedule which lists types of records, and the length of time they should be retained based on business needs. The retention policy can be found at the Information Management site within Library services.

6. Enforcement

6.1 Breaches of this policy may lead to disciplinary action, including dismissal for serious or repeated breaches. The University reserves the right to inform the appropriate authorities where conduct/actions may be unlawful.
### Appendix A - Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data owner</strong></td>
<td>An entity that can authorise or deny access to certain data, and is responsible for its accuracy, integrity, and timeliness. This is most commonly delegated to the Head of Unit.</td>
</tr>
<tr>
<td><strong>Data Protection Act (DPA)</strong></td>
<td>The Act regulates the use of “personal data”.</td>
</tr>
<tr>
<td><strong>Freedom of Information Act (FOIA)</strong></td>
<td>The Freedom of Information Act provides rights of public access to information held by public authorities.</td>
</tr>
<tr>
<td><strong>Central University Storage</strong></td>
<td>Storage made available by the Open University IT department, typically available through network drives or collaboration tools.</td>
</tr>
</tbody>
</table>